Amendments to the Specification

Please replace the paragraph on page 26, beginning on line 5, with the following amended paragraph:

Certain components are depicted in Fig. 2 for certain preferred embodiments of the methods and systems disclosed herein. In a preferred embodiment, as depicted in Fig. 2, event data or events 230 may be captured that reflects the use of a user interface 210. The agent 208 can capture the events 230 and transmit the events 230 through the network 112 to a server, which may be a secure server 214. A software agent 218 may be installed within the server 214 to facilitate application of a rule engine 222 to identify events, such as security events or policy events. The rule engine 222 may interface with a data facility 224, such as a database in which captured event data has been compiled and stored. Events 230 may be aggregated and processed, and reports 228 may be generated from the data facility 224, such as by conventional database reporting facilities. In embodiments, through use of a security process 220, such as installed on the secure server 214 or another server or machine that provides access to the data facility 224, various reports 228 in various configurations may be selectively accessed by individuals of varying status. For example, a manager ~~102~~202 may have visibility of events 230 solely within his or her department 108, while an information technology administrator 114 may have access to data procured from across the network 112. Alternatively, an executive of an organization may be privy to information of a personal nature input from users while an administrator may be provided access to only selective portion, or to aggregated statistical data, or to data for which personal identifiers have been obscured or discarded.

Please replace the paragraph on page 27, beginning on line 1, with the following amended paragraph:

High-level steps for capturing and reporting on events are depicted in the flow diagram 300 of Fig. 3. At a step 302, an event, such as a user accessing an Internet chat room, may be

detected. Capturing the event 302 can trigger a rule engine at a step 304, such as when the event is sent by the agent 208 to the server ~~314~~214 for operation by the rule engine 222. The rule engine 222 can store rules for operating on events of various types. At a step 308 the rule engine 222 can determine whether a particular event triggers a rule of the rule engine 222. If at the step 308 it is determined that an event triggers a rule, then the rule is executed at a step 310. For example, if the event has been previously defined as an unauthorized activity within a rule engine, then evidence of the event, and related temporal, user, and device information may be sent with an alert, such as an email message, such as to the manager ~~102~~202 or system administrator ~~114~~214. If at the step 308 the event does not trigger an alert rule, then the event may be stored at a step 312, such as in the data facility 224. Then, at a step 314 the system may report the event, either on its own or as part of an aggregated report, such as a report of all users who have accessed a particular Internet site, or other similar report. Thus, in addition to a report, an alert, proffered through electronic mail, a paging device, telephone auto-dialing, an SMS message or otherwise, may be generated and transmitted. Alternatively or in addition to sending an alert, the event data may be retained within a data facility 224 for subsequent data mining or processing.

Please replace the paragraph on page 38, beginning on line 4, with the following amended paragraph:

In a preferred embodiment, as represented by Fig. 10, a software agent 208 may be installed on a user computer 204. Such agent 208 may collect usage data 1008 from a user computer 204 and route such data, or a portion or aggregation thereof 1014, through a computer network 100. The agent 208 may perform various data organizing operations on the data including binning, clustering, application of regression or other statistical techniques, or any other method of cataloging, organizing, or efficiently storing or transmitting the data. Data collected by an agent may be stored within database tables or otherwise within a database such as the data facility 224 associated with the server 214 or optionally on user computers. In embodiments the agent 208, or a portion thereof, may reside on multiple user machines

204, and a portion of the agent ~~218~~208 may reside on a server 214 or other device connected to the network 100.

Please replace the paragraph on page 45, beginning on line 4, with the following amended paragraph:

Reports or selective views of output may be generated and categorized. For example, as depicted in the graphical user interface 2100 shown Fig. 21, security events 2102 and policy events 2104 may be monitored and displayed for occurrence ("Event Occurred") 2108, non-occurrence ("NO Event") 2110, or event disablement ("Event Disabled") 2106. A report may also indicate whether notation of the event has been viewed or emailed ~~2106~~. Color coding in the graphical user interface 2100 can help the viewer, such as a manager 102, quickly assess what security events may have occurred, so that attention can be paid to those events, rather than paying attention to a host of data that does not reflect any problem. A wide range of security events 2102 and policy events 2104 can be displayed for a manager 102 to review. For example, among security events 2102, the system may detect a system file change 2112, creation of a system director 2114, installation or setup of an application 2118, addition of a new user 2120, presence of an inactive user on the network 2122, detection of the downloading of a file 2124, status of an event log 2128, change in the status of the agent 2130, detection of backdoor activity 2132, detection of known exploit port activity 2134, adding a new computer to the system 2138, presence of an inactive computer on the system 2140, packet sniffer detection 2142, or modem usage or network properties 2144. Various policy events 2104 can also be detected, such as use of an inappropriate program 2148, use of a windows editor or policy editor program 2150, detection of abnormal desktop time 2152, detection of the status of the enterprise logon or logoff policies 2154, detection of unregistered users from the logon server 2158, detection of inappropriate content 2160, violation of Internet time usage policies 2162, or violation of concurrent licensing usage policies 2164. Each of the security events listed above can be reflected with a status indicator in a graphical user interface, such as to show that an event occurred 2108, such as by displaying a red circle or

similar symbol next to a listing of the security event in the graphical user interface. If no security event 2102 or policy event 2104 has occurred of a given type, then a green symbol 2110 or similar symbol can indicate that no such event occurred. A different symbol can indicate that detection of a particular type of event has been disabled.

Please replace the paragraph on page 53, beginning on line 21, with the following amended paragraph:

Referring to Fig. 39, in certain embodiments of the present invention, a system similar to the system 100 may be deployed in a hospital environment 3900. In embodiments, a hospital may include a hospital computer system ~~3914~~3904 with conventional elements, such as a network (or multiple networks) 112, one or more servers 3914, and various client devices 3904. The hospital environment 3900 and computer system may support one or more applications, including conventional applications such as financial or word processing applications, as well as applications specific to health care. For example, a patient record keeping application 3908 may be deployed on the hospital system, such as on a client device of a user, such as a doctor, nurse or administrator and on the server 3914. The record keeping application may operate on patient records 3910, which may be stored in a hospital database 3924. In such a situation, the hospital system 100 can be used to determine what users interacted with the patient record keeping application 3908 at what times using what machines 3904. In addition, the system 100 can capture keystroke data to determine what characters were entered when a user interacted with the patient record keeping application 3908, such as to record when a user on a particular machine entered a particular patient's name. The agent 208 of the system 100 captures, bins, and stores the usage data according to the principles of the invention described above, so that the system 100 can report, such as to the hospital administrator, what users interacted with a given patient record at what time. With such a report, an administrator can determine, for example, if attempts have been made to access a record from an unauthorized machine or by an unauthorized user.

Please replace the paragraph on page 59, beginning on line 11, with the following amended paragraph:

Referring to Fig. 42, in certain embodiments of the present invention, a system 4200 similar to the system 100 is deployed in a school or educational environment. In embodiments, a school or educational environment may include a computer system 4200 with conventional elements, such as a network 112, one or more servers 214, and various client devices 204. The system 4200 may support one or more applications, including conventional applications such as e-mail and word processing applications, as well as other conventional applications such as Internet browsers which are commonly used by both students and teachers for research and other educational projects. The system 4200 may include, deployed on the user machines 204, the servers 214, or both, one or more conventional or custom-developed educational applications 4208, such as applications for word processing, research, drawing, mathematical modeling, photography, making presentations, storing and manipulating data, storing and manipulating images, storing, playing and manipulating media, such as music, video, speech and sound, communications within and outside the environment, tracking student records, tracking student information, tracking health-related information, tracking family information, tracking information relating to testing, including standardized testing, tracking information relating to applications for admission, tracking information relating to honors, scholarships and awards, tracking information relating to participation in activities, tracking information relating to graduation and alumni, and many other applications. The system 4200 can allow an authority within the educational environment, such as a principal, dean, teacher, superintendent, administrator, professor, graduate student, librarian, scientist, department chairperson, or the any other such authority to monitor computer and application usage by individual users, by departments, or by the educational institution as a whole. For example, a standard Internet browser application 4214 may be deployed on the school system ~~4100~~4200. In such a situation, the system ~~4100~~4200 can be to analyze student usage and/or teacher usage over time increments and at the keystroke level to analyze whether behavior represented isolated incidents which may have been due to inadvertent acts or whether keystroke behavior reported to the system ~~4100~~4200 reflects repeated non-compliant behavior

such as actual reading of illicit or pornographic content, repeated visits to or extended time spent visiting a website promoting school violence or terrorism, or the like.

Please replace the paragraph on page 60, beginning on line 12, with the following amended paragraph:

In embodiments, the invention may be used in a school environment where the school needs proof about user activity, such as for CIPA 7 requirements of student appropriate computer use. The system can be set to store user input data for one year in the archive in the data storage facility ~~2244~~4224. During the school year the data can be made available for analysis and reporting. After the school year the data can be automatically removed.

Please replace the paragraph on page 62, beginning on line 15, with the following amended paragraph:

Referring to Fig. 43, in certain embodiments of the present invention, a system 4300 is deployed in a military or secure government environment. In embodiments, a military or secure government environment may include a computer system 4300 with conventional elements, such as a network (or ~~multiple~~military networks) 114, one or more servers 214, and various client devices or user computers 204. The system 4300 may support one or more applications, including conventional applications such as e-mail and word processing applications, database software, software for data capture and data mining, and middleware that integrates the various legacy systems, multi-agent systems, and other hardware and software that exist in the typical military environment. In particular, middleware (e.g. the Co-Abs Grid) may be deployed on the military system in order to integrate the operation of various networks, software, and hardware. The system 4300 may include one or more databases 4324, such as containing information, including records 4310 that relate to military applications. Because deployment of the system 4300 can occur by the agent 208, which can be deployed on the user computers 204, network 112 and servers 214, and because the system 4300 can collect keystroke data at the kernel level, it is particularly well suited to monitor security breaches on an integrated, multi-agent system. As with the use cases described

above, the system 4300 can be used to analyze personnel usage over time increments and at the keystroke level to analyze whether behavior represented isolated incidents which may have been due to inadvertent acts or whether keystroke behavior reported to the system 4300 reflects repeated non-compliant behavior such as actual reading of restricted files or databases, repeated visits to or extended time spent visiting a restricted database, or subsequent keystroke behavior indicating contact with outside third parties, downloading of classified information, etc.